Audit van IT en van het IT-auditberoep

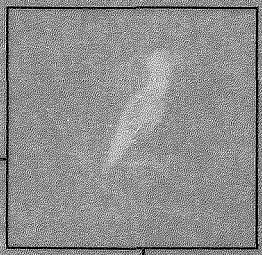
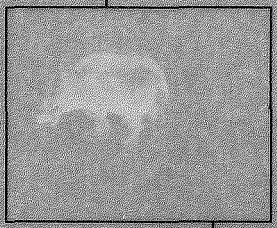
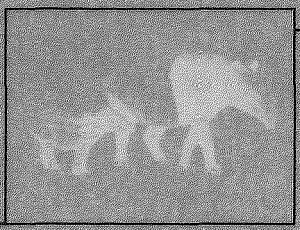
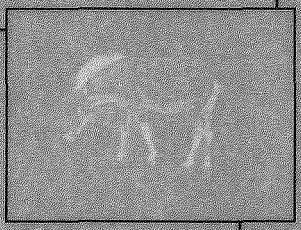
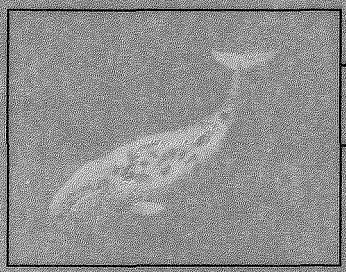
van Biene-Hershey, M.E.

2004

document version
Publisher's PDF, also known as Version of record

Mw. prof. M.E. van Biene-Hershey RE

Audit van IT en het IT-auditberoep

vrije Universiteit amsterdam

Prof. M.E. van Biene-Hershey RE

Audit van IT en van het IT-auditberoep

Publicatie ter gelegenheid van haar afscheid als hoogleraar EDP-audit aan de faculteit der Economische Wetenschappen en Bedrijfskunde van de Vrije Universiteit Amsterdam op maandag 8 november 2004.

Colofon

edp@feweb.vu.nl

Ontwerp: AVC Amsterdam 17078

Inhoudsopgave

1 Inleiding

De maatschappij is sterk afhankelijk van automatisering (IT), dat wil zeggen geautomatiseerde informatiesystemen (IT-toepassingen) en de onderliggende technische infrastructuur (IT-technieken). Veel meer afhankelijk dan onze maatschappij bereid is te erkennen.

De stelling van deze publicatie luidt: *"De maatregelen ter interne controle en beveiliging van IT zijn onvoldoende voor veel van de huidige en voorgenomen toepassingen daarvan en daardoor loopt de maatschappij onaanvaardbare risico's door het geheel van bekende en onbekende tekortkomingen in de IT".*

Deze stelling wordt onderbouwd door enkele structurele tekortkomingen in de IT te beschrijven. Vanuit de beroepsmatige plicht van een IT-auditor met betrekking tot de natuurlijke adviesfunctie[1] zijn vervolgens een aantal aanbevelingen gegeven die de risico's zouden kunnen beperken tot een aanvaardbaar niveau.

Uitgangspunt van dit betoog is het gebruik van IT in grote en middelgrote organisaties in zowel het bedrijfsleven als de overheidsector. Voor persoonlijk IT-gebruik, in het bijzonder voor privé-doeleinden, zijn de bedreigingen van de te behandelen tekortkomingen ook aanwezig, maar de maatschappelijke impact van calamiteiten bij deze laatste categorie is van een andere orde. Daarom komt persoonlijk IT-gebruik slechts zijdelings aan bod.

De huidige IT-producten die als fundament moeten dienen voor toekomstige ontwikkelingen kennen inherente bedreigingen die deze IT-producten in veel gevallen ontoereikend maken. De IT-auditor is mede debet aan deze omstandigheden. Immers, de belangrijkste toegevoegde waarde die een IT-auditor in de samenleving heeft, is zijn/haar onpartijdige perspectief en de deskundigheid waarmee hij/zij de organisatie ondersteunt. Indien de eisen en normen die de organisatie zelf daaraan stelt ontoereikend zijn, dan betekent dat niet dat de IT-auditor vrijuit gaat. Neen, de IT-auditor is - vaktechnisch gezien - verplicht zijn/haar deskundigheid te gebruiken om eisen en normen van de organisatie af te wijzen en duidelijk te maken waarom deze als uitgangspunt ontoereikend zijn voor de toekomstige IT.

---

[1] NOREA Jaarboek: *Reglement Gedrags- en Beroepsregels Register EDP-auditors, artikel 1.*

Vanzelfsprekend hoort bij elke negatieve bevinding (vaststelling van een tekortkoming) een advies over de wijze waarop een geïdentificeerd risico tot een aanvaardbaar niveau kan worden teruggebracht (de natuurlijke adviesfunctie).

Deze zwakke dienstverlening door IT-auditors heeft gevolgen voor het IT-auditberoep die niet onbesproken kunnen blijven. Een beroep dat onvoldoende is geëquipeerd voor haar beroepsuitoefening is op zich al een bedreiging.

De onderbouwing van de stelling vindt plaats in hoofdstuk 3 'Tekortkomingen'. In hoofdstuk 4 geef ik een aantal adviezen om de risico's als gevolg van de geconstateerde tekortkomingen te beperken. Hoofdstuk 5 bevat een beschouwing over domeindenken. Deze publicatie is afgerond met een korte conclusie en een dankwoord.

2 Terminologie

Voor de meeste definities van de gehanteerde terminologieën wordt verwezen naar 'NOREA geschrift N°. 1, IT-auditing aangeduid'[2] dan wel de richtlijnen en reglementen van de NOREA[3]. Deze definities zijn ook consistent met de definities zoals deze zijn te vinden in 'Handboek EDP-auditing' van Kluwer BV[4].

Om de waarnemingen te kunnen toetsen zijn normatieve uitgangspunten gewenst. Voor dit betoog zijn de normatieve uitgangspunten als volgt:

- Verschillende IT-toepassingen vereisen ieder hun eigen stelsel van beheersingsmaatregelen voor interne controle en beveiliging.

- Wettelijke bepalingen moeten bij de inrichting van IT worden meegenomen.

- Er zijn minimaal vier lagen die moeten worden onderscheiden bij het consistent en consequent implementeren van interne controlemaatregelen en beveiligingsmaatregelen (zie figuur 1).
  Het betreft:
  - fysieke relaties van het IT-product met de omgeving (deze omgevingsfactoren worden buiten beschouwing gelaten);
  - factor mensen en de personele organisatie waarbinnen zij functioneren;
  - informatiearchitectuur van IT-toepassingen en processystemen;
  - IT-technieken die worden gebruikt in de technische infrastructuur (waarin naast hardware ook programmatuur ter directe ondersteuning van de hardware wordt begrepen).

- De organisatie is volkomen afhankelijk van IT voor wat betreft de effectiviteit, efficiëntie, exclusiviteit, integriteit, beheersbaarheid, continuïteit en controleerbaarheid van alle bedrijfsactiviteiten.

- De IT-producten zijn geheel met elkaar geïntegreerd. Binnen een organisatie is er geen sprake van IT-toepassingen die geheel geen IT-interface (IT-technische relatie) hebben met andere IT-toepassingen binnen de organisatie. Deze interfaces moeten dusdanig zijn ingericht

---

2 NOREA geschrift N°.1, *IT-auditing aangeduid*, juni 1998.

3 NOREA Jaarboek, *Statuten, reglementen en richtlijnen.*

4 Handboek EDP-auditing, *1200 - Inleiding Uitgangspunten en 1300 - Inleiding Onderzoeksobjecten, een uitwerking van de domeinen*, afl. 24, augustus 2003, Kluwer.

dat ze de effectiviteit, efficiëntie, exclusiviteit, integriteit, beheersbaarheid, continuïteit en controleerbaarheid van de geautomatiseerde processen versterken.

- De reikwijdte van het begrip organisatie is vanuit een IT-perspectief bepaald door de reikwijdte van de technische infrastructuur, inclusief de (IT-)interfaces met juridisch onafhankelijke organisaties.

- Via telecommunicatie zijn er elektronische verbindingen binnen en tussen organisaties. Denk hierbij aan verbindingen tussen:
  - medewerkers van de eigen organisatie;
  - medewerkers van de eigen organisatie en andere organisaties;
  - medewerkers van de eigen organisatie en bekende en onbekende natuurlijke personen buiten de organisatie;
  - computersystemen zonder tussenkomst van mensen.

- In de ambtsaanvaardingsrede[5] bij mijn aantreden als hoogleraar sprak ik over IT-audit ten behoeve van het management. De EDP-Audit Opleiding van de Vrije Universiteit richt zich op IT in grote organisaties. De IT-auditor dient dan ook geëquipeerd te zijn voor de ondersteuning van dit management.

- Domeinen zijn volgens Van Dale Groot Woordenboek Hedendaags Nederlands[6] onder andere geestelijke gebieden. De IT-domeinen komen niet altijd overeen met duidelijk afgebakende IT-producten. Het is daarom verstandig ervan uit te gaan dat een domein binnen de IT-wereld eigenlijk virtueel (geestelijk) is. Immers, het is een afgebakende verzameling van zowel fysieke IT-producten als IT-processen, waarvan een aantal virtueel is. Deze verzameling moet leiden tot een herkenbare en functionele doelstelling van organisaties. Daaruit vloeit voort dat organisaties gelijksoortige eisen stellen aan de kwaliteitsaspecten exclusiviteit, integriteit, beheersbaarheid, continuïteit en controleerbaarheid. Bij het definiëren van een domein moeten ook de interfaces van dat domein met andere domeinen zodanig zijn gedefinieerd dat deze interfaces geen onaanvaardbare risico's inhouden voor het functioneren van dat domein.

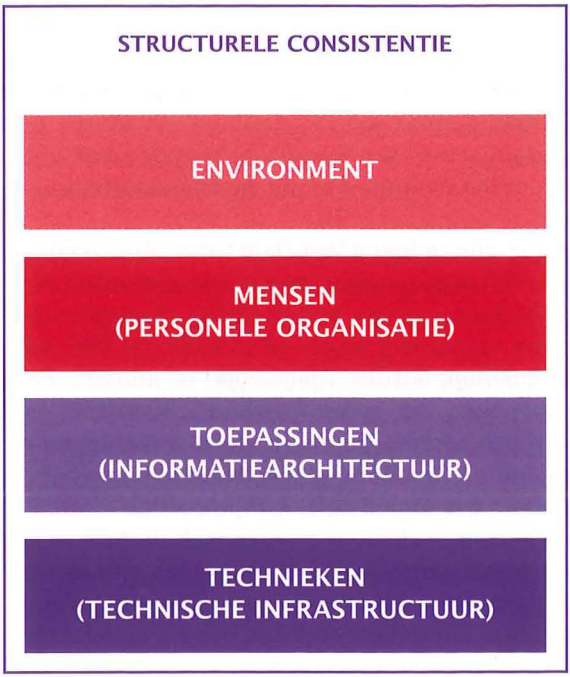
- Domeindenken in deze context is het ervoor zorgen dat een IT-domein een inherent en rationeel doel heeft en dat de interfaces van

5 M.E. van Biene-Hershey, *EDP-Auditing in relatie tot management*, Vrije Universiteit 1989.
6 Van Dale Groot Woordenboek, *Hedendaags Nederlands*, Versie 2.0, Van Dale Lexicografie bv, 2002

het IT-domein consistent zijn ontworpen om dit te waarborgen. De interfaces met andere domeinen moeten aan beide kanten consistent zijn met de doelen van de beide domeinen. Ieder domein kent vier generieke niveaus van interfaces, zoals weergegeven in figuur 1. Structurele consistentie van de vier lagen en de interfaces daartussen binnen een specifiek domein is ook een vereiste.

Het NOREA-geschrift 'IT-auditing aangeduid' behandelt ook domeinen. Deze domeinen worden gedefinieerd met het doel de reikwijdte van het vakgebied IT-auditing af te bakenen. In deze NOREA-publicatie is de doelstelling van het domeindenken het ondersteunen bij een verantwoorde inrichting van IT binnen een grote organisatie.

Figuur 1 Structurele consistentie



3 Tekortkomingen

Matrix 1 laat de relatie zien tussen de in dit hoofdstuk behandelde tekortkomingen en de belangrijkste kwaliteitsaspecten die door deze tekortkomingen worden bedreigd. De ernst van iedere bedreiging is situatieafhankelijk. Dat er sprake kan zijn van specifieke ernstige bedreigingen met betrekking tot een kwaliteitsaspect is voldoende reden om een tekortkoming in relatie tot dat kwaliteitsaspect te veronderstellen.

Matrix 1 Relatie tussen tekortkomingen en kwaliteitsaspecten

BEDREIGD KWALITEITSASPECT / TEKORTKOMING	Effectiviteit	Efficiëntie	Exclusiviteit	Integriteit	Beheers-baarheid	Continuïteit	Controleer-baarheid
1. Kwetsbaarheden voor virussen en dergelijke		Ja	Ja	Ja	Ja	Ja	Ja
2. Gebrek aan inzicht in de technische infrastructuur	Ja	Ja	Ja		Ja	Ja	
3. (Te) ingewikkeld sleutelbeheer			Ja		Ja		
4. Gebrek aan kwaliteitscontrole, in het bijzonder bij outcourcing	Ja	Ja		Ja		Ja	
5. Onvoldoende aandacht voor programmeertalen	Ja	Ja	Ja	Ja	Ja	Ja	Ja
6. Te veel detectieve en correctieve maatregelen				Ja	Ja	Ja	Ja
7. Gebrek aan inzicht in de totale informatiearchitectuur	Ja	Ja	Ja	Ja	Ja	Ja	
8. Het IT-auditberoep is onvoldoende geëquipeerd	Ja	Ja	Ja	Ja	Ja	Ja	Ja

3.1 Kwetsbaarheden voor virussen en dergelijke

De meest voor de hand liggende tekortkoming die op dit moment leidt tot onaanvaardbare risico's betreft de kwetsbaarheid van de technische infrastructuur voor aanvallen via internet. Men spreekt over virussen, wormen, denial of service attacks et cetera en steeds komen nieuwe verschijningsvormen erbij.

Belangrijk is te vermelden dat de deskundigen het erover eens zijn dat de aard en de ernst van deze aanvallen toenemen. Tijdens recente aanvallen zijn niet alleen nieuwe technieken waarneembaar om onze netwerken en systemen te verstoren, maar ook nieuwe strategieën. Zonder

vervanging van de TCP/IP-protocollen is het niet uit te sluiten dat vroeg of laat een aanval zal plaatsvinden met desastreuze gevolgen voor onze samenleving[7].

Voor organisaties betekenen deze tekortkomingen in het TCP/IP-protocol extra beveiligingsinvesteringen, aanslagen op de continuïteit van de dienstverleningen en vervolgens een gebrekkige controleerbaarheid van de verleende diensten. Vanzelfsprekend is het binnendringen en ongewenst gebruik van IT-producten een bedreiging voor de exclusiviteit en integriteit van de data.

3.2 Gebrek aan inzicht in de technische infrastructuur

Gebrek aan inzicht in de technische infrastructuur in relatie tot de IT-toepassingen die daarmee worden ondersteund, leidt tot verborgen beveiligingsrisico's. Ter bevestiging van deze stelling dient men te denken aan het feit dat de meeste audits van de inrichting van autorisatieprofielen voor het bevoegde gebruik van IT-producten (in samenhang met de authenticatiemethoden) leiden tot de conclusie dat er ernstige tekortkomingen zijn in de logische toegangsbeveiliging van de onderzochte organisatie. Zoals prof. dr. I.S. Herschberg zo vaak stelde: de complexiteit van het geheel van IT-producten, waarmee kennis van het systeem wordt bemoeilijkt, geeft een vals gevoel van veiligheid. Slechte beheersing van het bevoegde gebruik van IT-producten bedreigt hoofdzakelijk de exclusiviteit.

Beveiligen is bedoeld voor het beschermen van waarden. Veel organisaties hebben veel geld uitgegeven om hun IT adequaat te beschermen. Een significant deel van dat geld was niet nodig als bij het ontwerp en de realisatie van de gebruikte besturingssystemen en de daarmee samenhangende telecommunicatieprotocollen voldoende aandacht was geweest voor interne controle en beveiliging.

Zonder inzicht in de totale samenhang van de technische infrastructuur kan een organisatie de effectiviteit, efficiëntie en beheersbaarheid van de technische infrastructuur niet aantonen. Calamiteiten met betrekking tot de continuïteit van de IT-ondersteuning vormen het meest herkenbare symptoom dat impliciet aangeeft dat alles beter zou moeten zijn geregeld.

Bijna alle beveiligingsmaatregelen zijn gericht op detectie en correctie.

[7] R. Pethia, Director CERT Coordination Center, Carnegie Mellon University, Pittsburgh PA, USA, Presentation at International CYBER Security Syposium 21 & 22 August 2003.

De meeste preventieve maatregelen met betrekking tot beveiliging zijn te vergelijken met het innemen van vitaminen om te voorkomen dat je ziek wordt. De oorzaak van de bedreiging, waarvoor de beveiliging noodzakelijk is, wordt niet weggenomen.

Omdat organisaties IT-producten aanschaffen die niet adequaat zijn voor de doelen waarvoor de organisatie de IT-producten wil gebruiken, moet apart worden geïnvesteerd in maatregelen om de risico's van de tekortkomingen te beperken. Zou de leverancier van deze producten verantwoordelijk moeten worden gesteld voor de ondeugdelijkheid van zijn producten? IT-auditor, waar ben je als beslissingen worden genomen om ondeugdelijke IT-producten aan te schaffen?

3.3 (Te) ingewikkeld sleutelbeheer

Ten eerste vormt de complexiteit van de sleutelbeheerprocedures op zichzelf al een bedreiging voor de integriteit van cryptografische technieken die steunen op deze sleutels.

Ten tweede vormt de veelheid van wachtwoorden die men moet onthouden een bedreiging voor de exclusiviteit van het gebruik van die wachtwoorden. Wachtwoorden zijn alle authenticatiemiddelen die uitsluitend steunen op kennis en niet op bezitskenmerken.

- Er zijn zoveel wachtwoorden die men moet onthouden en vele worden maar zeer sporadisch gebruikt. Dus, men schrijft deze op een papiertje en verliest dat vervolgens, of men maakt alle persoonlijke wachtwoorden hetzelfde. Het overvloedige gebruik van wachtwoorden is geen oplossing. Het is onbeheersbaar.

- Wachtwoorden zijn geen effectief middel indien accountability ook een vereiste is voor de handelingen. De term 'accountability' heeft niet alleen te maken met de eis van eenduidige legitimatie, maar heeft ook te maken met het achteraf verantwoordelijk kunnen stellen van individuen voor gedane zaken. Het middel voor authenticatie moet dus zo sterk zijn dat het redelijk is aan te nemen dat het desbetreffende individu de enige is die de daden kan hebben verricht, dan wel iemand anders de gelegenheid heeft gegeven tot het verrichten van de daden. Wachtwoorden zijn dus ontoereikend als beveiligingsmiddel indien er sprake is van een verantwoordelijkheidsstelling achteraf.

De integriteit van het sleutelbeheer is bijna niet te waarborgen in een normale organisatie. Het opzetten van een adequate inrichting voor sleutelbeheer conform erkende standaarden is namelijk zeer ingewikkeld. Een continue werking conform de opzet is waarschijnlijk te veel gevraagd van een gewone organisatie.

Let wel, er zijn veel meer kritische kanttekeningen te plaatsen bij sleutelbeheer, bijvoorbeeld bij de keuze van de encryptietechniek en de sleuteldistributieprocedures.

3.4 Gebrek aan kwaliteitscontrole, in het bijzonder bij outsourcing

Gebrek aan aandacht voor de verantwoordelijkheid voor kwaliteitscontrole op uitbestede IT-diensten leidt tot een verzwakking van de effectiviteit en efficiëntie (en in veel gevallen de integriteit en continuïteit) van de dienstverlening door de uitbestedende organisatie.

In deze tijd van kostenbesparing wordt outsourcing van ontwikkelingsafdelingen en rekencentra gezien als een manier om inefficiënties in de organisatie te beperken en dus kosten te besparen. Als de eigen verantwoordelijkheid in relatie tot de uitbestede diensten adequaat wordt ingevuld (informatiestrategie, kwaliteitsbeheersing, service level management), dan worden de kostenbesparingen niet meer zo significant.

Dus de enige echte reden voor outsourcing is het verbeteren van de kwaliteit van de IT-dienstverlening (effectiviteit). Eenvoudig gezegd, laat het over aan een organisatie die beter gekwalificeerd is dan de eigen organisatie. Door de sturing en controle op die kwaliteit te veronachtzamen, zal deze over enige tijd ernstige tekortkomingen gaan vertonen.

In organisaties met een zeer hoge afhankelijkheid van geïntegreerde IT is het niet mogelijk om alle IT-ondersteuning uit te besteden. Het blijft voor een organisatie de vraag of outsourcing beheers-technisch gezien effectiever is of niet.

3.5 Onvoldoende aandacht voor programmeertalen

Het schrijven van programma's is nog steeds ambachtelijk en niet elke hogere programmeertaal is geschikt voor gebruik bij het ontwikkelen van iedere IT-toepassing. De noodzaak om kritischer te zijn bij de keuze van een (hogere) programmeertaal voor het ontwerpen en uiteindelijk definiëren van de operationele code, wordt onderschat. Mode schijnt

meer te heersen dan verstand. Vraagstukken, zoals toekomstige onderhoudbaarheid, vervangingskosten en integriteitseisen met betrekking tot de broncode van programmatuur in productie, zijn onderwerpen die niet systematisch worden beoordeeld bij de keuze van een ontwikkelingstaal. Hierdoor moeten vraagtekens worden gezet bij de beheersbaarheid, integriteit, effectiviteit en efficiëntie van de informatiesystemen.

Bij sommige programmeertalen kan tevens niet meer worden vertrouwd op de controleerbaarheid van de werking van IT. Zo is er bijvoorbeeld een geval uit het verleden bekend waarbij een satelliet niet goed in een baan om de aarde kwam als gevolg van programmafouten. Deze fouten waren eigenlijk te wijten aan het gebruik van een programmeertaal die niet accuraat genoeg was. De softwareproblemen met de Amerikaanse raket naar Mars hadden natuurlijk ook te maken met programmafouten. Er wordt gesproken over onvoldoende stabiliteit van de gebruikte programmeertaal dan wel het in onvoldoende mate testen van de programmatuur.

Noch de IT-auditopleidingen noch de IT-opleidingen besteden voldoende aandacht aan de programmeertalen en de wijze waarop adequaat controle op het eindproduct moet plaatsvinden. 'Upper case' en 'lower case tools' hebben de integriteit van de code verbeterd. Maar het is nog steeds niet mogelijk om zonder 'add-ons' de gegenereerde code in productie te nemen.

Veel ontwikkelingen van systemen worden gedaan in programmeertalen die niet berekend zijn op de eisen die door een comptabele IT-toepassing worden gesteld aan interne controle en beveiliging. Nog vaker is waar te nemen dat IT-toepassingen worden ontwikkeld in programmeertalen die uiteindelijk niet onderhoudbaar blijken. Hierdoor komt de continuïteit van de IT-toepassing in het geding.

3.6 Te veel detectieve en correctieve maatregelen

Het gebrek aan preventieve maatregelen binnen de professionele IT-afdelingen is een onaanvaardbare bedreiging van de integriteit en exclusiviteit van IT-toepassingen, omdat detectiemechanismen niet of te laat werken. Dit is ook een bedreiging voor de controleerbaarheid.
Het gebruik van sommige programmeertalen kan de vereiste preventieve maatregelen ondermijnen. Indien hoge eisen worden gesteld aan het stelsel van beheersmaatregelen voor interne controle en beveiliging van

een IT-toepassing of aan een onderdeel van de technische infrastructuur, dan worden de functiescheidingen tussen de ontwikkel-, acceptatie- en productieomgeving onvervangbare preventieve maatregelen. Dit geldt dus niet alleen voor het in productie nemen van IT-toepassingen, maar ook voor elke technische wijziging in de IT-technieken.

Twee voorbeelden waarbij het is misgegaan:

- In het verleden hebben systeemontwikkelaars in Nederland kans gezien creditcardnummers te stelen, doordat het hen werd toegestaan dat zij op het productiesysteem, gedurende productiewerkzaamheden, ook ontwikkelwerkzaamheden uitvoerden. Dit leidde tot exclusiviteitsverlies.

- In de Verenigde Staten is er een schandaal geweest rondom de geautomatiseerde stemmachines in de staat Georgia. Dit voorbeeld betreft het vermengen van het ontwikkelen en tegelijkertijd accepteren en invoeren van informatiesystemen. Het geheel leidde tot twijfels over de integriteit van de leverancier. Zelfs de overheid van de staat Georgia werd verdacht van politieke manipulaties. Dit raakte de controleerbaarheid, integriteit en beheersbaarheid van de IT-toepassing.

Bij de ontwikkeling van informatiesystemen wordt de functiescheiding tussen de ontwikkelaar en de opdrachtgever soms verwaarloosd. Met het gebruik van standaardpakketten is de functiescheiding sterker. Echter, bij de noodzakelijke aanpassingen van het aanvullende maatwerk wordt de vereiste functiescheiding tussen opdrachtgever en ontwikkelaar niet meer in acht genomen. Kortom, er is te weinig begrip voor het belang van integere programmacode (en dan bedoel ik de code die door de computer wordt uitgevoerd).

3.7 Gebrek aan inzicht in de totale informatiearchitectuur

Informatiearchitecturen die niet expliciet worden beheerd veroorzaken ongewenste tekortkomingen op het gebied van exclusiviteit en integriteit van de informatievoorziening.

Het allegaartje van de informatiearchitectuur is onbeheersbaar, kost te veel aan onderhoud en de complexiteit van vernieuwingen wordt onderschat waardoor deze te lang duren en soms zelfs mislukken. Dit leidt tot bedreigingen ten aanzien van de beheersbaarheid, continuïteit, efficiëntie en effectiviteit van de IT-toepassingen. In veel gevallen hebben de

oplossingen voor millenniumproblemen het geheel alleen maar ondoorzichtiger gemaakt en dus nog moeilijker te beheersen.

De vlucht naar SAP en andere ERP's is een ander bewijs voor deze stelling. ERP's dwingen een totale informatiearchitectuur af. Het is voor veel organisaties een aantrekkelijke oplossing voor de 'brei' die hun informatiearchitectuur is geworden. Maar ERP's kennen ook bedrijfsrisico's:

- Afhankelijkheid van de leverancier.
- Onvermijdbaar verval van software (deterioration), waardoor een organisatie minder efficiënte programmatuur in productie moet nemen dan de oude versie/release.
- Te veel koppelingen tussen bestaande IT-toepassingen en de ERP leiden uiteindelijk tot ongewenste kosten bij migraties naar nieuwe releases van de ERP.
- Ontoereikende en ontbrekende functionaliteit moet door de organisatie worden opgevangen, wat leidt tot efficiëntieverliezen en mogelijk ook tot problemen met de integriteit van de informatievoorziening.

En dan moeten de ingeslopen redundanties natuurlijk niet worden vergeten. Deze ten behoeve van de flexibiliteit ingebouwde redundanties leiden enerzijds tot hogere ontwikkelingskosten en operationele kosten en anderzijds tot een bedreiging van de integriteit van de informatievoorziening. Een bekend probleem in dit kader is de noodzaak om meerdere releases van een databasemanagementsysteem operationeel te houden, omdat niet alle ontwikkelaars in staat zijn de nodige veranderingen in de informatiesystemen tijdig aan te brengen om gelijktijdig over te kunnen gaan op de nieuwe release van het databasemanagementsysteem.

Zonder een goede informatiearchitectuur waaraan de ontwikkeling van nieuwe IT-toepassingen, wijzigingen in bestaande IT-toepassingen en het beleid ten aanzien van interne controle en beveiliging kan worden getoetst, wordt de initieel aanwezige samenhang van IT-toepassingen verstoord en het geheel onbeheersbaar.

3.8 Het IT-auditberoep is onvoldoende geëquipeerd

Het wetenschappelijke gehalte van IT-auditing in de praktijk is onvoldoende. Iedereen herdefinieert begrippen, creëert 'buzzwords' en er is te weinig aandacht en erkenning voor de schaarse min of meer vastgestelde definities van IT-onderwerpen en terminologie in het IT-auditvakgebied.

De NOREA heeft slechts drie richtlijnen met betrekking tot de uitvoering van IT-audits: de eerste is Opdrachtaanvaarding, de tweede is Dossiervorming en de derde is Rapportage. Tevens is er een richtlijn met betrekking tot permanente educatie. Het door een RE voldoen aan deze richtlijn bepaalt of een RE als gekwalificeerde IT-auditor mag optreden. Geen van deze richtlijnen raakt de wijze waarop een audit dient te worden uitgevoerd. De afspraken over terminologie zijn bovendien zeer marginaal.

Deze gebrekkige normstelling wordt vaak verdedigd met de opmerking dat er zo weinig zaken voor de Raad van Tucht van de NOREA zijn geweest of met de vraag waarom de NOREA opnieuw het wiel moet uitvinden. Echter, zonder voldoende richtlijnen en reglementen, ontbreken de mogelijkheden om een beroep te doen op de Raad van Tucht. Hoe kan men weten of andermans wielen toereikend zijn als men geen idee heeft over de eisen die men zelf stelt aan de eigen wielen?

Gebrek aan heldere richtlijnen, erkende toetsingscriteria, consensus over vereiste niveaus van interne controle en beveiliging en gebrek aan voldoende IT-kennis kunnen leiden tot het beeld dat gekwalificeerde IT-auditors zichzelf onvoldoende serieus nemen.

Tenslotte dient een IT-auditor de effectiviteit van de organisatie te dienen door bij te dragen aan het verminderen van de risico's met betrekking tot exclusiviteit, integriteit, continuïteit en controleerbaarheid van de dienstverlening. Bovendien moet hij/zij aantoonbaar kunnen bijdragen aan een efficiëntere organisatie.

4 Adviezen

Bij dit hoofdstuk kan matrix 2 worden gehanteerd om de relaties te overzien tussen de te behandelen adviezen en de tekortkomingen zoals aangegeven in hoofdstuk 3.

Matrix 2 Relatie tussen de tekortkomingen uit matrix 1 en de adviezen

ADVIES \ TEKORTKOMING	1	2	3	4	5	6	7	8
1. Ontwikkel domeindenken voor interne controle en beveiliging	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
2. Dwing adequate ontwerpcriteria af voor de technische infrastructuur	Ja	Ja	Ja		Ja	Ja	Ja	
3. Respecteer de preventieve maatregelen die nodig zijn bij professionele IT-activiteiten		Ja	Ja			Ja	Ja	
4. Toets operationele domeinen op criteria vanuit het domeindenken	Ja	Ja	Ja		Ja	Ja	Ja	
5. Third Party Mededelingen en Certificeringen	Ja	Ja	Ja	Ja	Ja		Ja	Ja
6. Maatschappelijke betekenis van IT-auditing duidelijk plaatsen		Ja		Ja			Ja	Ja

4.1 Ontwikkel domeindenken voor interne controle en beveiliging

Ten behoeve van het bepalen van de vereiste IT moet men domeinen definiëren die zich onderscheiden door verschillen in toetsbare parameters voor interne controle en beveiliging. Vanuit dat domeindenken kan men vervolgens bepalen welk type hardware, systeemprogrammatuur en IT-toepassing in ieder domein moet/mag worden geplaatst. Dit document zal dan dienen om investeringsvoorstellen voor technische infrastructuur en IT-toepassingen te toetsen alvorens de investering goed te keuren. Beleid ten aanzien van programmeertalen die mogen worden gebruikt bij systeemontwikkelingen dienen per domein expliciet te worden gemaakt. Dit domeindenken zal ook IT-auditors ondersteunen bij hun audits en adviezen.

Binnen de organisatie zal het domeindenken bijdragen aan de beheersing van de ontwikkelingen in de technische infrastructuur en de informatiearchitectuur[8].

[8] NOREA, *IT Governance, een verkenning*, Casus KPN, juni 2004.

De weg om dit te bereiken kan als volgt zijn:

- Overheden en standaardisatie-instituten definiëren generieke domeinen en leggen de functionele eisen voor deze domeinen vast, inclusief de interfaces met andere domeinen.

- Organisaties bepalen de eigen eisen en wensen met betrekking tot domeinen en selecteren de generieke domeinen die het best passen bij hun eisen.

- IT-producenten bouwen IT-producten specifiek voor bepaalde generieke domeinen en laten die producten daarop certificeren.

- Organisaties selecteren de IT-producten uit de selectie van gecertificeerde producten voor het generieke domein dat het best past bij de behoefte van de eigen organisatie.

De organisatie zal toch aanpassingen of additionele maatregelen moeten treffen, maar dan kan men verwachten dat het om marginale aanpassingen zal gaan.

4.2 Dwing adequate ontwerpcriteria af voor de technische infrastructuur

Organisaties moeten IT-technieken eenvoudig kunnen toepassen binnen de technische infrastructuur, zonder noodzaak van uitgebreide en/of additionele investeringen in maatregelen ter interne controle en beveiliging. Belangrijke ontwerpcriteria die in ieder geval moeten worden gehanteerd voor controleerbare en veilige technieken en de interfaces daartussen, worden in de bijlage samengevat.

IT-technieken moeten gecertificeerd zijn voor verantwoord gebruik in bepaalde generieke domeinen.

4.3 Respecteer preventieve maatregelen nodig bij professionele IT-activiteiten

Vanuit het perspectief van interne controle en beveiliging zijn er vier fundamentele maatregelen die adequaat moeten zijn ingericht om de integriteit van een operationele informatievoorziening te waarborgen:

- Volledige scheiding tussen ontwikkel- en acceptatieprocessen en tussen het acceptatieproces en de operations van de productiesystemen (technisch beheer, changemanagement en operationeel beheer). Deze scheidingen waarborgen de voortdurende integriteit van de operationele processen.

- Access control (maatregelen om bevoegd gebruik te waarborgen): op een toereikende wijze ingericht en in productie genomen, zodat alles is gewaarborgd behalve de meest inhoudelijke controles op de integriteit van gegevens.

- Aard van de taal waarin men systemen ontwikkelt: deze is consistent met de vereiste functiescheidingen tussen opdrachtgever, ontwikkelaar, exploitatieorganisatie en gebruiker.

- Authenticatietechnieken voor het verlenen van toegang tot systemen mogen geen inherente bedreiging zijn voor deze functiescheidingen.

Bovendien moet bij IT-toepassingen waarbij mensen accountable worden gemaakt, de technische infrastructuur waarborgen dat er sprake is van een onafhankelijke en integere logging (vastlegging) van alle systeemactiviteiten. Let wel, de eisen aan de authenticatietechniek wegen hier ook zwaarder.

4.4 Toets operationele domeinen op criteria vanuit het domeindenken

Een vereiste bij deze toets is de actieve controle en IT-audit van:

- Inrichting van domeinen.

- Toetsing van nieuwe ontwikkelingen en investeringen aan de normen van de domeinen.

4.5 Third Party Mededelingen en Certificeringen

Het afgeven van Third Party Mededelingen is gewenst bij organisaties waaraan IT-dienstverlening is uitbesteed en ten aanzien van internet-serviceproviders. Dit is echter niet verantwoord zolang de normstellingen niet helder en toegankelijk zijn voor alle belanghebbenden. Hierbij moeten natuurlijk ook de minimumeisen aan de auditaanpak algemeen aanvaard zijn.

Van belang voor de kwaliteit van IT in een organisatie zijn een professionele aanpak en documentatie van uitgevoerde audits. Deze audits dienen te leiden tot het certificeren van systemen als voorwaarde voor het operationaliseren ervan. Indien een organisatie - en de maatschappij - afhankelijk wordt/is van de IT-diensten, dan wordt een onafhankelijk oordeel met een goedkeurende strekking noodzakelijk, voordat wordt overgegaan tot invoering van het systeem binnen het domein waarin het systeem operationeel wordt gemaakt.

4.6 Maatschappelijke betekenis van IT-auditing duidelijk plaatsen

In de toekomst zal wettelijke erkenning nodig zijn. Voor een fervent tegenstander van een wettelijke bescherming van de IT-auditfunctie is dit een vreemde uitspraak. Belangrijkste reden om nog steeds tegen te zijn, is de overtuiging dat IT-auditors hiervoor (nog) niet klaar zijn. Toch is het duidelijk dat het in de toekomst wel nodig zal zijn. Het belang van IT voor de maatschappij zal zodanig toenemen dat IT-auditing wettelijk moet worden erkend om organisaties te beschermen tegen inadequaat uitgevoerde audits.

De overheid en het bedrijfsleven zullen waarschijnlijk eerst een calamiteit nodig hebben voordat ze zullen inzien dat ze druk moeten uitoefenen op de IT-auditberoepsgroep om haar huis op orde te brengen.

5 Domeindenken

Een domein heeft een in brede kring erkend doel en dit betreft een rationeel doel. Om over een domein te kunnen spreken is een duidelijke afbakening van het domein en zijn omgeving noodzakelijk.
Op het moment dat een afbakeningsconcept wordt geïntroduceerd, komt ook de verplichting om de interacties met de wereld om het domein heen te bepalen, zodanig dat rekening wordt gehouden met de specifieke eisen van dat domein. De echte onbetwiste voorbeelden van domeinen, zoals landen, gevangenissen en bankkluizen, hebben procedures en maatregelen om interacties met de wereld om zich heen te regelen.

Op basis van het voorgaande kan niet worden gesteld dat onze PC's (en dit geldt ook voor veel grotere computers) geen domeinen (kunnen) zijn. Helaas moet dit met een dubbele ontkenning worden uitgedrukt. De oorzaak van de onduidelijkheid over deze IT-domeinen ligt in het feit dat IT-professionals tot nu toe slechts één soort domein hebben gedefinieerd. Dit is namelijk het 'general purpose'-domein. Maar een 'general purpose'-domein is geen domein met een specifiek doel. Hierdoor creëren organisaties ieder voor zich en tot op zekere hoogte specifiekere doelen voor hun domeinen. Vandaar dat organisaties de noodzaak voelen om additionele maatregelen te treffen op het gebied van interne controle en beveiliging. Veel organisaties kennen bijvoorbeeld nu al productiedomeinen, testdomeinen, ontwikkeldomeinen en end-user-domeinen.

De noodzaak om afspraken te maken over de vorm en inhoud van de interfaces van het domein met de wereld om zich heen, vloeit voort uit de aard van een domein. Verreweg de meeste IT-interfaces worden gebouwd vanuit het principe 'any to any' en de organisatie die het aanschaft moet zorgen voor de noodzakelijke beperkingen in deze 'any to any'-situatie. Domeindenken is dus echt nog niet ontwikkeld.

Het mondiale gebruik van IT is te vergelijken met een dierentuin. De verschillende gebouwen en terreinen waarin de dieren zijn gehuisvest zijn de domeinen (en daarbinnen subdomeinen) met bijpassende controle, afgestemd op de mate waarin de dieren onderling en met mensen interactief kunnen zijn (de interfaces). Echter, bij het mondiale IT-gebruik zijn de domeinen en interfaces lang niet zo goed geregeld als bij dierentuinen. De oorzaak hiervan is dat de gebouwen - dat wil zeg-

gen de domeinen - niet zijn toegesneden op de eisen van de inwoners - de gebruikers van de domeinen. Er is geen sprake van consistent ontworpen domeinen over de vier lagen heen (zie figuur 1 op blz. 8).

Een domein met duidelijk omschreven doelen voor de organisatie zal zijn samengesteld uit IT-toepassingen en IT-technieken die niet meer en zeker niet minder beveiligd en controleerbaar zijn dan door het domein wordt geëist.

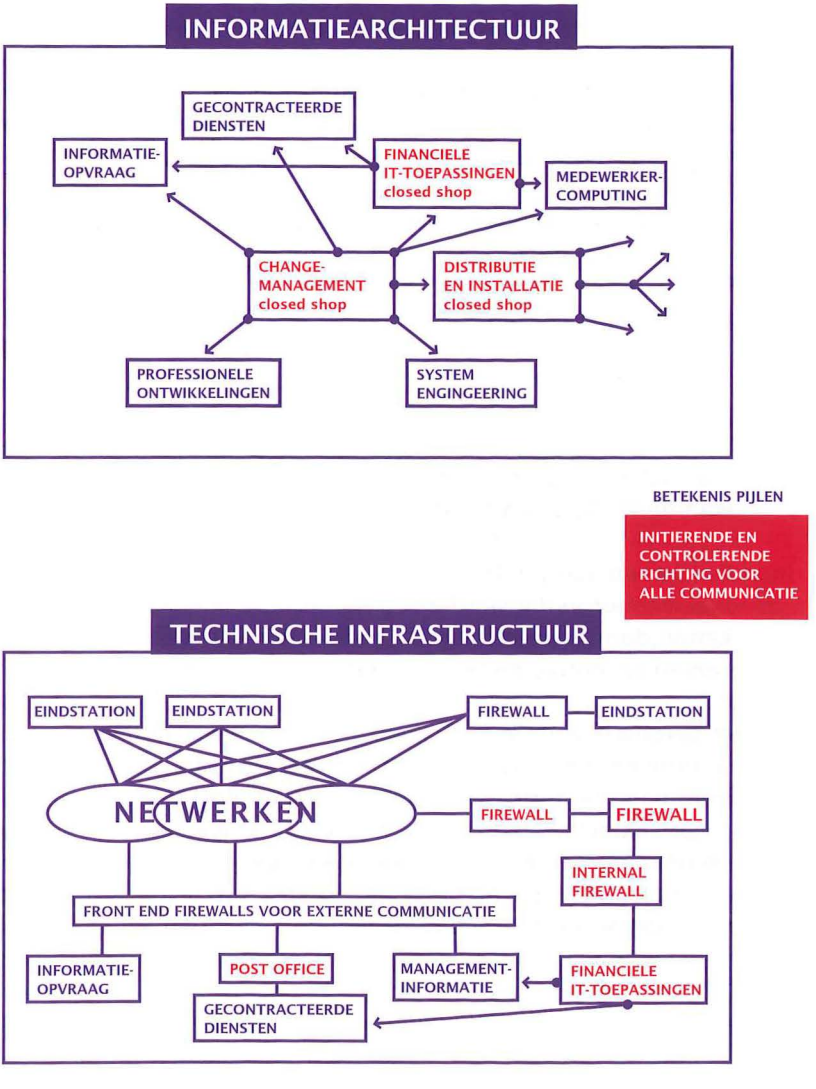
Het is nodig om generieke domeinen te bepalen met omschreven niveaus van access control, authenticatievereisten, integriteitcontroles, maatregelen ter beheersing van het domein, continuïteitsmaatregelen en mogelijkheden voor de benodigde controleerbaarheid. Nadat deze generieke domeinen zijn bepaald, kunnen IT-productontwikkelaars producten ontwerpen en vervaardigen die aan de criteria van een specifiek generiek domein voldoen. Dit laatste is natuurlijk verifieerbaar en kan worden gecertificeerd.

Organisaties moeten hun informatiearchitectuur en technische infrastructuur ordenen naar de generieke domeinen om vervolgens veilige producten te kunnen aanschaffen. Een voorbeeld van het domeindenken dat tijdens mijn colleges is gebruikt, is afgebeeld in figuur 2. Een behandeling van de betekenis hiervan is gegeven in mijn boek 'IT-auditing, An object oriented approach[9].

Domeindenken en vervolgens het implementeren daarvan is heel moeilijk. Het bouwen van adequate IT-producten voor generieke domeinen leidt tot langere ontwikkeltijden en duurdere producten. Maar eenmaal iets ontwikkelen in plaats van meerdere malen hetzelfde ontwikkelen door iedere organisatie is wel aanzienlijk goedkoper. Helaas bewijzen de afgelopen 15 jaren dat er geen sprake zal zijn van een vrijwillige overstap door IT-producenten naar het bouwen van IT-producten voor generieke domeinen. Daar waar het bedrijfsleven systematisch verzuimt orde op zaken te stellen bij onderwerpen van maatschappelijk belang, moet de overheid ingrijpen. Dat is geen prettig vooruitzicht, gegeven het gebrek aan efficiëntie waarmee de overheid zich tot op heden bemoeit met IT.

[9] M.E. van Biene-Hershey, *IT Auditing, An Object Oriented Approach*, Chapter 4, 1996, digitaal verkrijgbaar bij de EDP-Audit Opleiding van de VU.

Figuur 2 Domeindenken



Als bewijs van deze stelling kan worden aangevoerd:

- Discussies over encryptie.
- Mentaliteit dat een wet voldoende is om iets te regelen (de veronderstelling dat beoordeling van opzet en bestaan voldoende is om een adequate werking af te dwingen).
- Onbegrip voor de noodzaak om voldoende tijd (en geld) te investeren om IT-toepassingen adequaat operationeel te maken.
- Bestaan van vrijwel uitsluitend wetgevingen gericht op criminele opsporingen. Dit gaat ten koste van wetgeving die een betere IT-kwaliteit afdwingen.
- Verzuimen een visie te ontwikkelen over de betekenis van IT in de maatschappij. Er wordt nu slechts gewerkt aan een visie over de wijze waarop IT de bureaucratie efficiënter kan maken.
- Ontbreken van juridische kaders om de IT-producenten verwijtbaar te maken voor verliezen die een organisatie maakt als gevolg van gebreken in door hun geleverde IT-producten. Dit kan helpen de IT-producenten te motiveren betere producten te leveren.

Het beroep IT-auditing zal alleen in het belang van de samenleving kunnen groeien indien wij, IT-auditors, veel agressiever dan op het ogenblik, aangescherpte normen en standaarden op deskundige wijze toepassen. Op het vaktechnische vlak betekent dit dat wij actief moeten helpen om generieke domeinen te ontwikkelen en deze te gebruiken als norm voor het toetsen van informatiearchitecturen en technische infrastructuren, zowel operationeel als in wording.

6 Conclusie

Storend is het feit dat iedereen de genoemde tekortkomingen erkent, maar deze tekortkomingen bagatelliseert. Er wordt niets structureel ondernomen om deze tekortkomingen te elimineren. Wachten totdat een calamiteit plaatsvindt is het pad dat nu bewust of onbewust wordt bewandeld. Daarom is het denken over de structuur van besturingssystemen en datacommunicatieprotocollen en IT-toepassingen aan herziening toe.

Vanuit generieke domeinen moeten ontwerpeisen worden gemaakt voor de besturingssystemen in samenhang met de communicatieprotocollen. De communicatieprotocollen moeten zodanig worden ontworpen dat communicatie tussen de verschillende domeinen verantwoord is. Hiermee kunnen organisaties de technische infrastructuren realiseren met bouwstenen die sterk genoeg zijn.

Vervolgens zullen de ERP's en andere IT-toepassingen zodanig moeten worden gestructureerd, dat hun functies inpasbaar zijn in de gedefinieerde generieke domeinen. Dit betekent dat de informatiearchitectuur van een ERP het mogelijk moet maken om op een inzichtelijke wijze de functies van de ERP in verschillende generieke domeinen te plaatsen.

De delegatie van bevoegdheden aan mensen in de organisatie (autorisaties) en aan cliënten moet zijn vastgelegd in access-control-systemen en moet met adequate authenticatiemiddelen zijn geïmplementeerd. Hiermee kunnen de functionele bevoegdheden van mensen in overeenstemming worden gebracht met de door hun raadpleegbare domeinen (en daarbinnen specifieke functies) die zij vanwege hun functie of hun relatie met de organisatie mogen benutten. Ook moeten de maatregelen met betrekking tot de fysieke omgeving in overeenstemming zijn met de eisen van het domein. IT heeft nu al een veel grotere invloed op de samenleving dan ooit tevoren. De gevolgen van disfunctionerende dienstverlening door een IT-serviceprovider zullen niet uitsluitend de winst van deze serviceprovider aantasten, maar ook het welzijn van al haar klanten.

IT-toepassingen zijn veel efficiënter geworden en er is een enorme toename in de verscheidenheid van IT-toepassingen. De groei in het gebruik is in belangrijke mate toegenomen door inventiviteit bij het bouwen van informatiesystemen en processystemen. Het vertrouwd

raken met de tekortkomingen kan mijn stelling niet ontkrachten. *"De maatregelen ter interne controle en beveiliging van IT zijn onvoldoende voor veel van de huidige en voorgenomen toepassingen daarvan en daardoor loopt de maatschappij onaanvaardbare risico's door het geheel van bekende en onbekende tekortkomingen in de IT".*

7 Dankwoord

Mijn ruim 41 jaar tellende loopbaan is altijd uitdagend en toekomstgericht geweest. De mensen waarmee ik heb mogen samenwerken, zowel in de IT- als de IT-auditwereld, waren net als ik mensen met echte liefde voor hun vak. Ik heb zeer veel geleerd van de collega Register Accountant. Ik sta bekend als iemand die zeer kritisch is over het accountantsberoep. Ja, dat ben ik wanneer ik waarneem dat ze te gemakkelijk denken te weten wat goed is voor het IT-auditberoep. Ik ben wel jaloers op de vaktechniek en de professionele instelling van de RA's die ik ken. Ik zou graag zien dat de IT-auditopleidingen al in staat waren om dergelijke kwaliteiten aan hun studenten over te brengen.

Dat Nederlands niet mijn moedertaal is, zal niemand zijn ontgaan. Bij IT-management en IT-auditing is effectieve communicatie bepalend. Ik heb hiervoor altijd een zware wissel moeten trekken op collega's. Het zijn er te veel om allemaal op te noemen.

Er zijn wel twee personen die ik in dit opzicht wil noemen: Marcel Bongers en Kai Hang Ho. Ik kan het aantal keren niet tellen dat Marcel bij het publiceren bereid was om mij te ondersteunen. Kai Hang wil ik nu ook danken voor zijn steun bij de totstandbrenging van dit afscheidscollege.

Ik wil ook Paul Harmzen danken. Net als Marcel ken ik Paul van ver voor de start van deze opleiding. Paul heeft samen met mij de workshops begeleid. Hij was altijd in staat om een verhitte discussie in het gareel te brengen. Onze basisuitgangspunten waren nagenoeg altijd gelijk. Echter onze wijze van uitleg vaak zeer verschillend. Dit gaf de goed luisterende student, hoop ik, iets om over na te denken.

Met al deze kritiek op IT en IT-auditing tijdens dit college en meer in het bijzonder in de uit te reiken publicatie, moet ik zeggen dat ik best trots ben op de opleiding die Hans de Lange, Ronald Paans en ik hebben mogen neerzetten. Ik vertrouw er op dat Hans en Ronald deze opleiding verder ontwikkelen en dat de opleiding in de toekomst nog beter zal worden dan vandaag de dag al het geval is.

Ik heb gezegd.

Bijlage

Alhoewel veel punten die in deze bijlage worden genoemd al lang bekend en toegepast zijn, worden deze punten niet altijd meegenomen bij het ontwerpen van IT-technieken. Daarom deze bijlage om de IT-auditor een soort van samenvatting te geven van belangrijke inrichtingscriteria:

- Besturingssystemen (en de hardware van computers):

  - Structureel afgedwongen onderscheid tussen programmatuur en gegevens;

  - Alle 'calling-protocols' moeten een standaardinterface hanteren;

  - Alle pointers in systemen moeten 'forward' en 'backward' pointers zijn;

  - Beheren van domeinen met veilige standaardprotocollen voor communicatie tussen die domeinen;

  - Voor de domeinen met de hoogste eisen aan interne controle en beveiliging moeten bijzondere eisen worden gesteld aan:
    -aard van de IT-toepassingen die operationeel mogen zijn in dat domein;
    -communicatieprotocollen en regels voor 'access control' die nodig zijn voor toegang tot dat domein;

- Communicatiesystemen inclusief, waar van toepassing, de hardware (alle technologieën):

  - Onderscheid maken tussen het transport van gegevens en het transport van programmacode (dit betekent een telecommunicatieprotocol dat uitsluitend gegevens dan wel programmacode aanbiedt aan een besturingssysteem van een domein);

  - Op modem- of nodeniveau een bescherming aanbrengen tegen ongeautoriseerde toegang;

- Melden aan de verzender indien een bericht niet volledig en/of juist bij de ontvanger is bezorgd;
- Gebruik van voldoende veilige protocollen over het gehele netwerk;

- Beschikking over verschillende niveaus van beveiliging om verschillende generieke typen domeinen te kunnen bedienen;

- Protocollen voor communicatie met domeinen die de hoogste eisen stellen aan interne controle en beveiliging:
  - Zorgen voor een volledige en juiste gegevensoverdracht;
  - Ervoor zorgen dat de verzender de routing van berichten kan bepalen;

  - Voorkomen dat berichten van een onbekende worden afgeleverd bij aangeslotenen die dat niet wensen (closed user groups);

  - Netwerk-node-controle die ervoor zorgt dat de uiteindelijke ontvanger uitsluitend berichten ontvangt die aan het beveiligingsniveau voldoen dat door de ontvanger is bepaald;

  - Te allen tijde gebruikmaken van voldoende veilige communicatieprotocollen;

  - 'Logging' van alle gegevenspakketten die over een node worden getransporteerd.